RSAC 2025 Conference

Many Voices.
One Community.

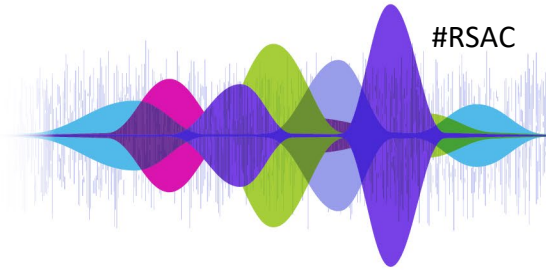
SESSION ID: APP-M03

Developer Centric and Layered Container Security - Lessons from the Trenches

Ken Atkins
Chief Architect
ADP

Seena Iype
Product Leader in AppSec
ADP

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

This presentation is for informational purposes only and should not replace professional advice or judgment. The views expressed are those of the presenters and do not necessarily reflect the views of ADP. ADP assumes no responsibility for the accuracy or completeness of the information in this presentation.

Who are We?

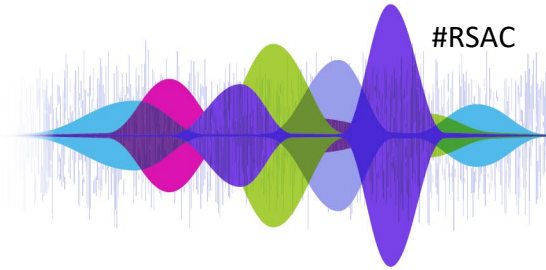
Ken Atkins

- Chief Architect for various security tooling applications and initiatives at ADP including:
  - ADP Container Security Initiative
  - ADP DevSecOps Workbench
  - Various Infrastructure AI initiatives
- 40+ years industry experience
  - 16+ years with ADP

Seena Iype

- Veteran Software developer and into Product Management for last 7 years
- Responsible for an inhouse Security Product for as part of the Developer Experience initiative
- Leading E2E strategy for Container Security
- Mentor with WiCys and AnitaB

Who is in the Audience



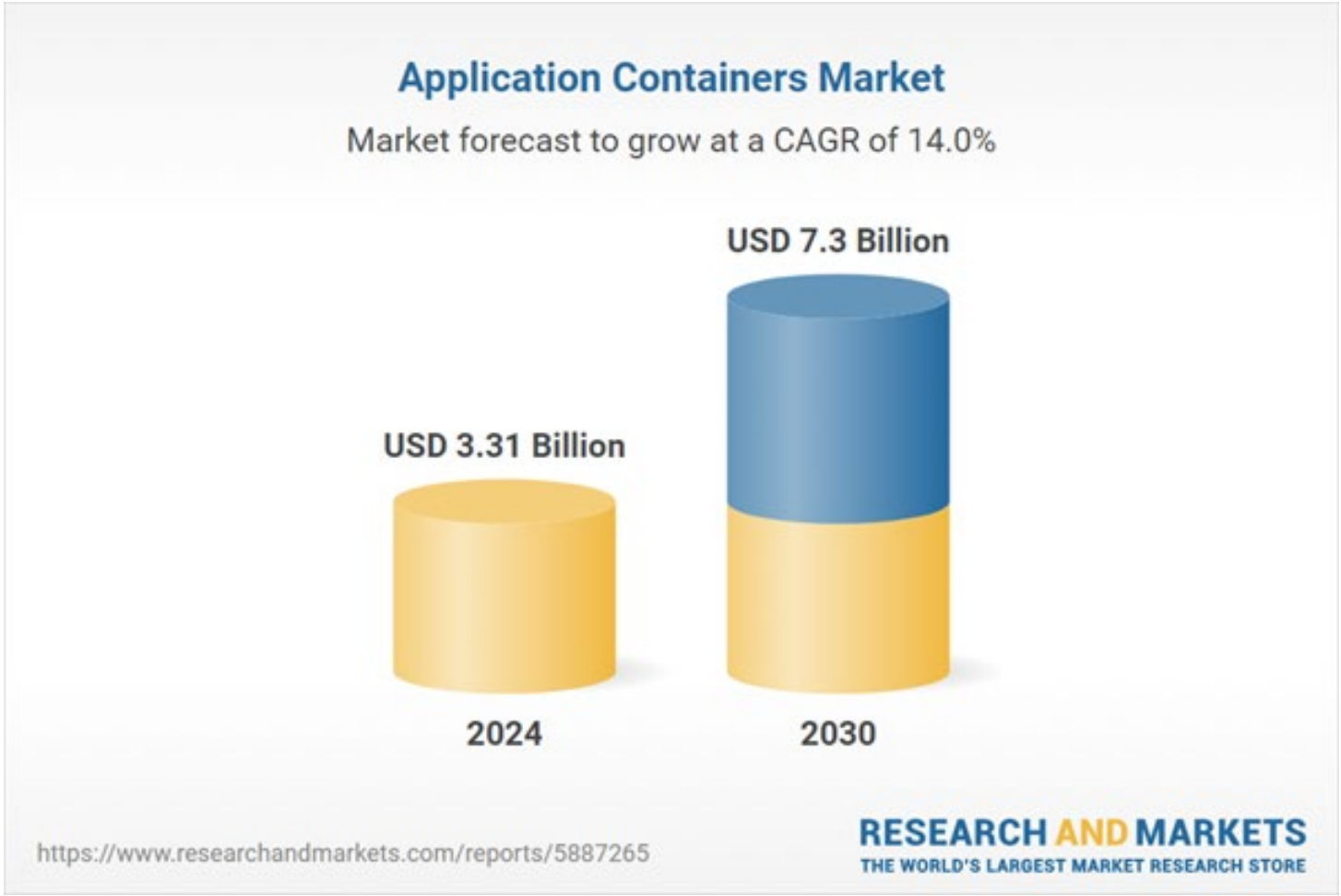
What is your Company Size?

Small < 100 developers
Medium < 1000 developers
Large < 3000 developers
XL > 3000 developers

What is your experience with Containers?

Not started yet, planning to start soon
Dipped our toes, last year
In the last 5 years
Beyond 5 years

Did you know?



The Application Containers Market grew from USD 2.91 billion in 2023 to USD 3.31 billion in 2024.

It is expected to continue growing at a CAGR of 14.00%, reaching USD 7.30 billion by 2030.

https://www.researchandmarkets.com/report/app-container?utm_source=GNE&utm_medium=PressRelease&utm_code=shhq5p&utm_campaign=2020056+-+Application+Container+Market+Trends+Analysis+Report+2024-2030%3a+Rising+Adoption+of+Containerization+Technology+in+Retail%2c+Healthcare%2c+and+Telecom+Spurs+Growth&utm_exec=chdomspi

Did you know?

- ~9 out 10 organizations had at least 1 container or Kubernetes security incident in the last 12 months

In the past 12 months, have you experienced any of the following impacts to your business as a result of containers/Kubernetes security or compliance issues or incidents?
53%
Project delays or disruptions
46%
Revenue or customer loss
30%
Fines, legal action, or lawsuits
26%
Employee termination

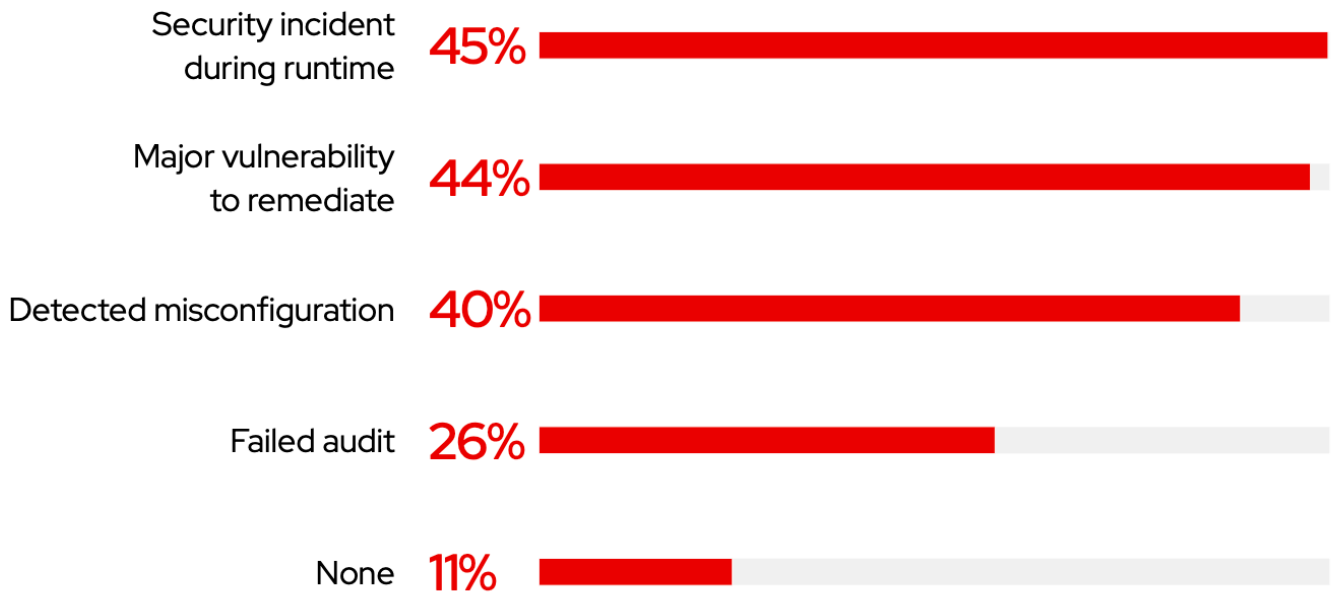
Red Hat

Q29. In the past 12 months, have you experienced any of the following impacts to your business as a result of containers/Kubernetes security or compliance issues or incidents? Base size: Total = 600

https://www.redhat.com/en/engage/state-kubernetes-security-report-2024

Did you know?

In the past 12 months, what security incidents or issues related to containers and/or Kubernetes have you experienced?



Red Hat

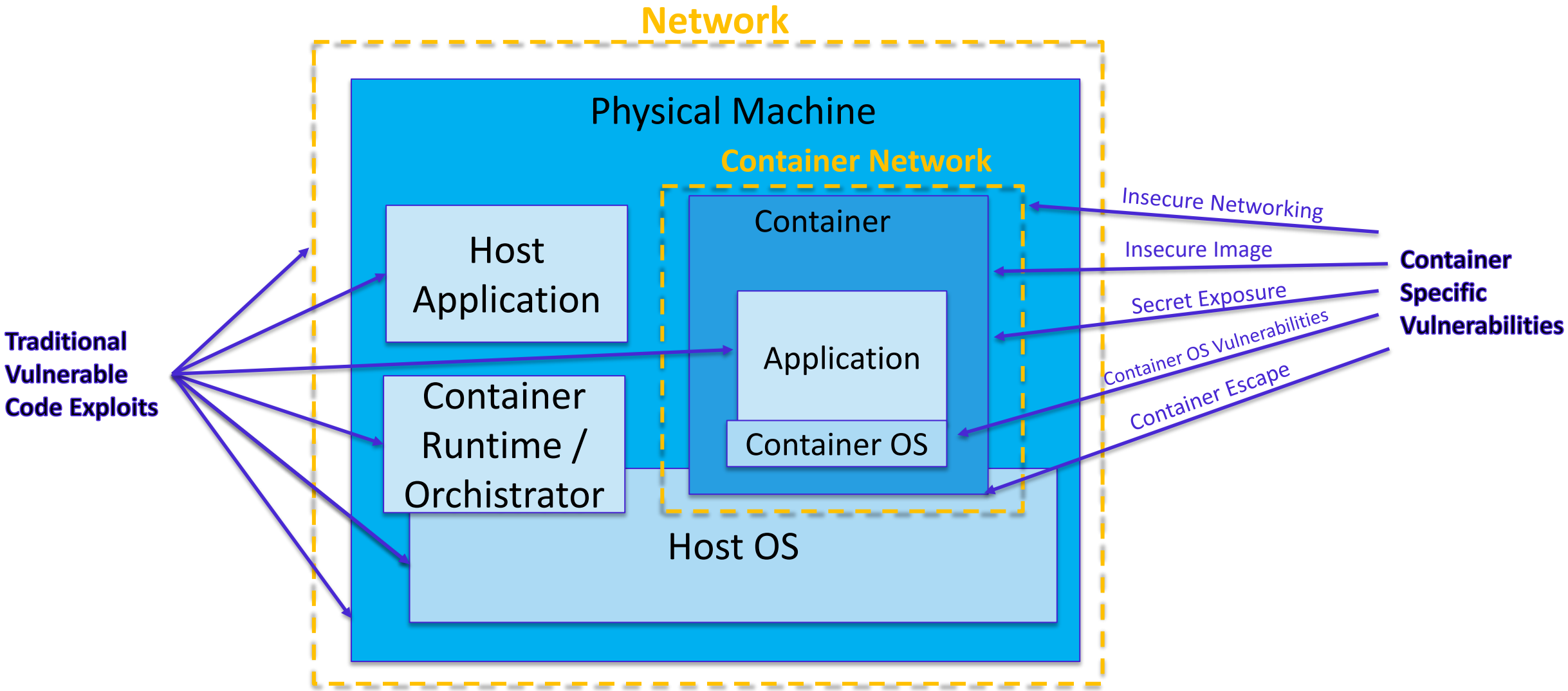
Q28. In the past 12 months, what security incidents or issues related to containers and/or Kubernetes have you experienced? Base size: Total = 600

https://www.redhat.com/en/engage/state-kubernetes-security-report-2024

Agenda

1. Overview of Container Ecosystem
   - Security scenarios
   - Architecture overview
2. Large Organization challenges
3. Container Security Initiative
   - Pillars for Container Security
   - Phases of implementation

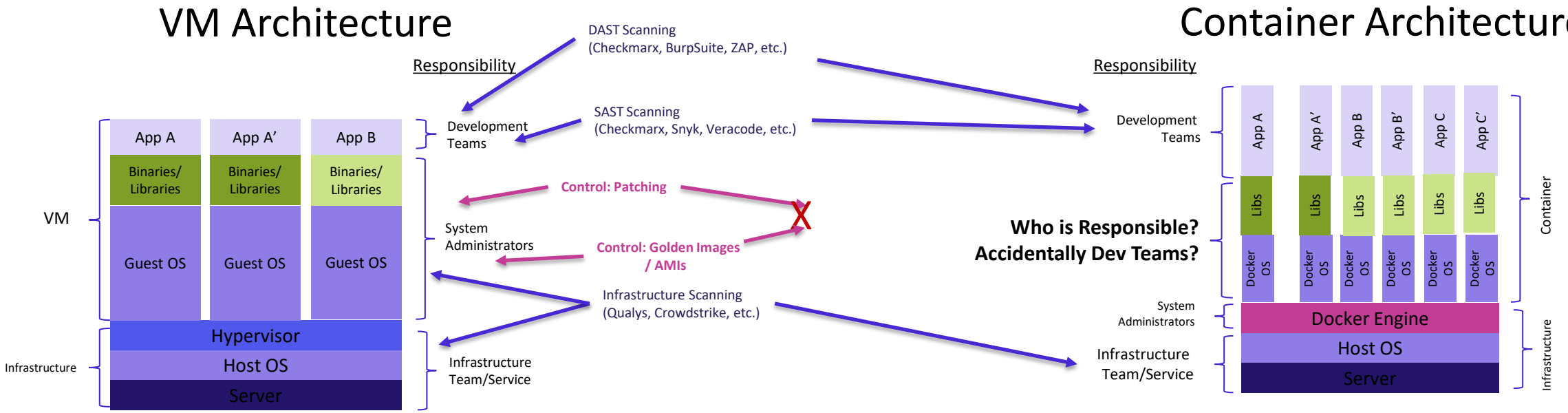
Container Security Challenges



RSAC 2025 Conference

Container Security Challenges

- Containers are different from “traditional” development architectures (for instance VMs)



- Container OS / Library Management left to developers
- Developers often do not have the skillset to manage this
- Lead to a “Hit it with a hammer until it works” mentality

- Who is responsible for the security of containers?
  - Developers? Security team? DevSecOps?

Lesson Learned at ADP: Need base Image curation and Hardening

Who are we? ADP

Providing tailored solutions that simplify work

ADP at a glance

1949 year founded

64,000 associates

1.1M+ clients worldwide

$19.2B USD revenue FY24

Serves clients in **140+** countries

30th year on the Fortune 500

No matter your business size, we've got you covered

1-49 EMPLOYEES

Small Business

Faster, easier, more reliable HR and payroll solutions designed to help you focus on what matters.

- Payroll →
- Professional Employer Organization (PEO) →
- Time & Attendance →
- Retirement →

MORE SMALL BUSINESS SOLUTIONS

50-999 EMPLOYEES

Midsized Business

Superior payroll solutions and HR tech designed to help you manage your entire workforce with ease.

- Payroll →
- Professional Employer Organization (PEO) →
- Time & Attendance →
- Retirement →

MORE MIDSIZED BUSINESS SOLUTIONS

1000+ EMPLOYEES

Large Business

Adaptable HCM designed to drive people performance and keep ahead of continual change.

- Integrated HCM →
- Payroll →
- Workforce Management →
- Retirement →

MORE LARGE BUSINESS SOLUTIONS

https://www.adp.com/

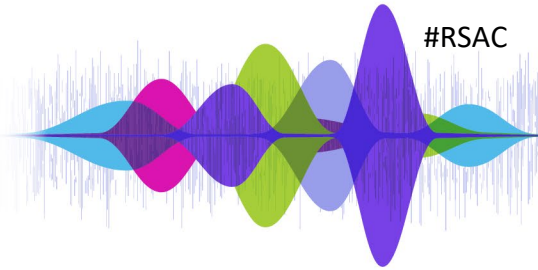
Large Organization Challenges

- >100s of separate products
- >100s of distinct development teams, >1000s of developers
- Distributed architecture standards and decision making
  - Each BU can set their own standards and processes
  - Resistance to non-functional initiatives
- Developers Attitude
  - I don't have time to do this, it does not add value
  - Developers: I am getting hit with too many non-functional requirements
  - I really don't understand container security ramifications.

Realization of the Problem in Large Organizations

- New technology gets ahead of security considerations
- Internal and external security audits may identify the potential problem
- Recommendation: Start a Container Security Initiative to address container specific security concerns
  - A part of the overall application security planning and maturation for the organization.

Container Security Initiative at ADP



- ADP Implemented a “Container Security Initiative”
  - ADP already has an extensive existing layered and comprehensive application security program that secures
- Cross Functional Team across ADP
  - Including: ADP Global Security Organization, Risk and Reliability Org, Global Infrastructure, Key development organizations
- Ken Atkins and Seena Iype were Core team members from the start

RSAC 2025 Conference

Container Security Initiative

Goals?

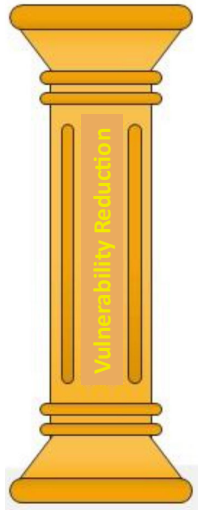
What if:

1. Time to Remediate (TTR) critical threats was couple of days
2. Ownership, Traceability and Control
3. Security by default, to help teams work on more innovation

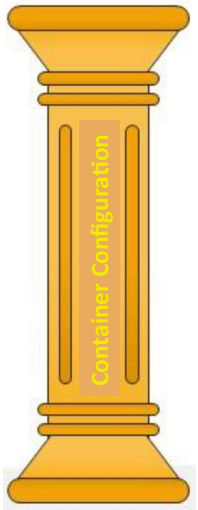
Note: Be Patient, it's going to take time....

Three Pillars

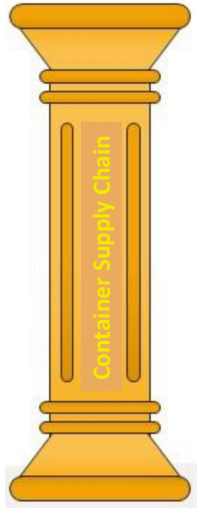
Container Security



Vulnerability Reduction (CVE, CVSS etc)



Configuration Issues (static and runtime)



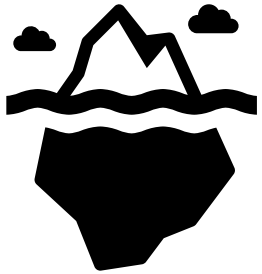
Supply Chain Issues (Provenance)
Internal generated Images
Vendor Images

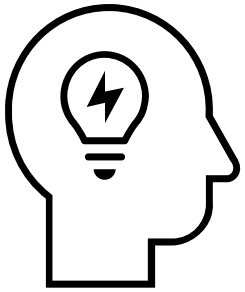
How to select where to start?

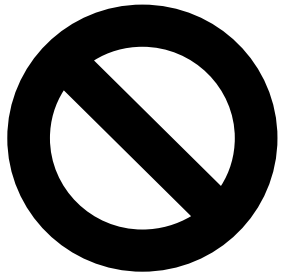
- Biggest Bang for the buck
- Easy adoptable solutions
- Development culture

Pillar selected – Vulnerabilities Reduction

Phased Approach







Phase 1 – Visibility of security issues (Run Time and Build Time)

Phase 2 – Provide easy solutions to foster remediation

Engagement, Communication

Phase 3 – Roll out and Enforcements – Audit, Enforce (Emerging ruleset)

RSAC 2025 Conference

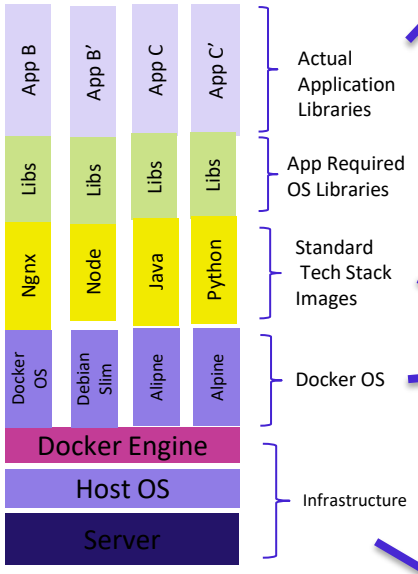
Phase 1 – Visibility to security issues

Phase 1 – Scanning & Visibility of Security issues

1. Identify vulnerability scanner to scan images
   - Open-source scanners
   - Vendor solutions
2. Gain Visibility to your security issues from Container images
   - Implement a Runtime vulnerability scanning process
     - Find all running containers running in any kubernetes environment and scan them
     - Distinguish between production and development/non prod environments
   - Shift Left – ability to scan in your CICD pipelines (where possible)
3. Reporting and scoring by application

Source of Container Vulnerabilities

Container “Layers”



Application introduces vulnerabilities from their library dependencies (i.e. Pipfile, requirements.txt, etc.)

Need to be addressed by Dev Teams

5-10% of Vulnerabilities

Applications often need additional OS libraries

Most docker images use “offical” Base images from tech community (i.e Python, Node, Java, etc.)

Can be addressed by “Hardening” base images

90-95% of Vulnerabilities

You probably already have established procedures for these

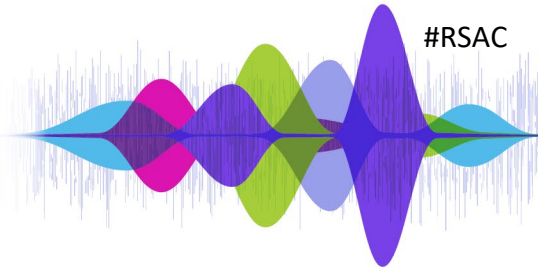
RSAC 2025 Conference

Phase 2 – Provide easy solution to foster remediation

Phase 2: Solution: "Hardened" Base Images

- How to remove base image vulnerabilities?
  - Option 1: Harden your own base images
  - Option 2: Vendor Solutions
- You should manage and update a repository of approved base images
  - Tag image life cycle (Supported, Deprecated, End of Life)
  - Who owns the base images?
- You should also use a Docker “Multi-Stage” build to reduce threats
  - (i.e. take shell script and other insecure tools out of final image)

Hardened Base Image Vendor Selection

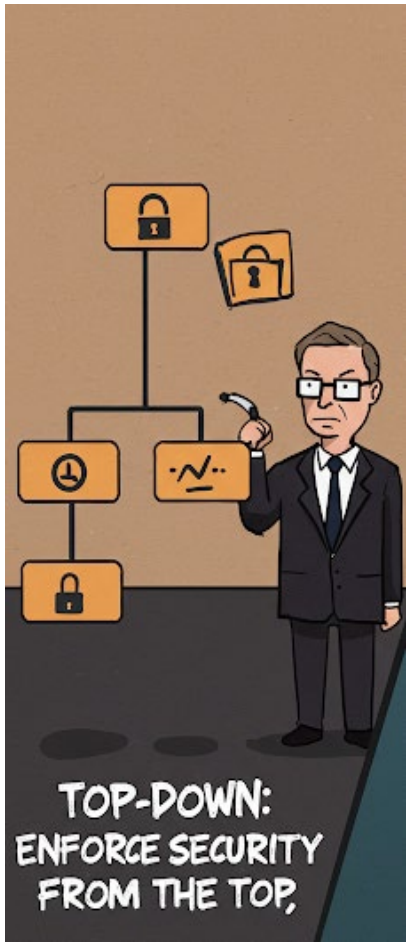


- Vendors take many approaches
  - Container Specific OS + Build from latest libraries
  - “Distro-less” OS (i.e. *very* minimal OS) + Build from latest
  - Work with maintainers to address critical issues quickly
- Ask what approach a vendor is taking
  - Some vendors only take 1 approach (leaving some vulnerabilities)
  - Some vendors take ALL approaches (and have basically 0 vulns)

RSAC 2025 Conference

Phase 3 – Rollout and Enforcements

Approaches in Large Org



Developer Centric Approach

IDENTIFY SOLUTIONS - VISIBILITY AND REMEDIATION

FIND INTERNAL CHAMPIONS AND PILOT WITH TEAMS (HONEST FEEDBACK)

PILOT TEAMS SHARE TO EXPERIENCE DEV COMMUNITY (SHARE THE EXCITEMENT)

ESTABLISH ONGOING SUPPORTIVE COMMUNITY (OFFICE HOURS, CHANNELS, TRAININGS...)

MONITOR AND MEASURE RISK REDUCTION AND SPOTLIGHT TEAMS

Carrot & Stick

- In large organizations it can be difficult to force adoption
- You need to provide easy solutions (The carrot)
- You still need to Measure, Rate, and monitor teams to ensure adoption (The stick)
- Phased Hard Enforcements

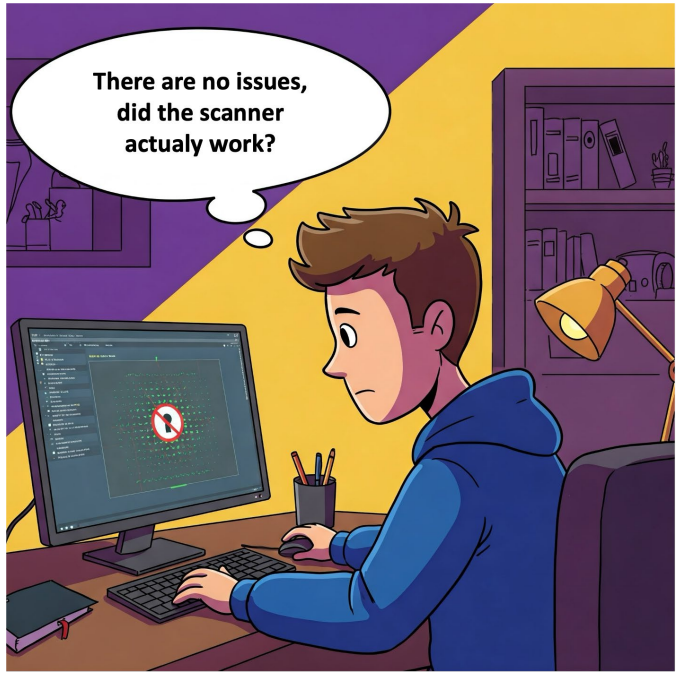
Actual Outcomes with Developers

- Risk Reduction
  - Developers often ask “Is this really a risk?” about CVEs
  - Ken’s Response: If you have zero CVEs, you KNOW there are no risks!

Actual Outcomes with Developers

- Engagement and Excitement within Dev Community

The Base Images were so good it surprised the developers

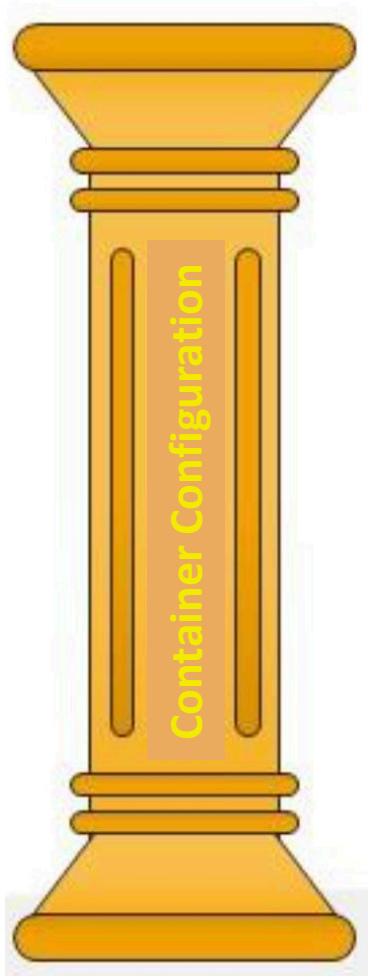


- Ownership not Deflection
- Relationships and Trust – Culture Shift (Security Mindset)

RSAC 2025 Conference

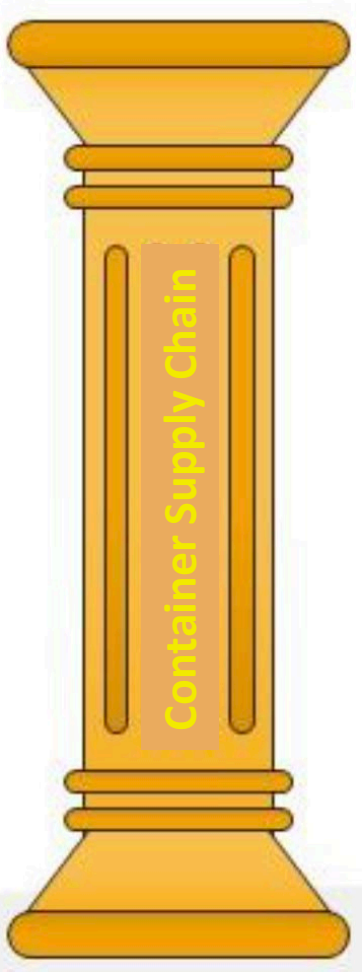
Other Pillars

2nd Pillar: Container Configuration



- Phase 1: Implement IAC and Runtime configuration scanning
- Phase 2: Developer Centric Solutions
  - Curated Base Images (already avoid many issues)
  - IAC Templates (for Kubernetes yaml, etc.)
- Phase 3: Monitoring, scoring, enforcement
  - Initially score and notify about configuration issues
  - Eventually block deployment of containers that don’t pass scans

3rd Pillar: Supply Chain



- Phase 1: Evaluation
  - Identify all container Delivery Pipelines
  - Identify all container repositories
- Phase 2: Developer Centric Solutions
  - Implement Standarized Container Repository (ies)
  - Implement Container signing process in all delivery pipelines
- Phase 3: Monitoring, scoring, enforcement
  - Initially notify development teams that they are using unsigned images
  - Eventually block deployment of unsigned images

RSAC 2025 Conference

Let's Review

Many Voices.
One Community.

Apply What you have learned today

- Next week:
  - **Reflect and Evaluate**
    - What is your Container Eco-System and security risk across layers look like?
    - What is your Development Culture and Challenges look like?
      - *PS: Be collaborative not adversarial*

- In the first three months following this presentation you should:
  - **Put together a Core Team :**
    - Discuss and decide on which pillar to start with
    - How to provide visibility to container security to the development teams?
    - Identify solutions that are easy to adopt by the development community

Apply What you have learned today

- Within six months you should:
  - **Developer Centric Roll out**
    - Provide visibility to dev community on the scale of the problem
    - Develop and Pilot solutions and Create excitement within the Development community
    - Align on metrics to reduce security risk (strategically)

PS: Save enforcement until complete visibility (less noise/false positives) and easy to implement solutions are in place.

RSAC 2025 Conference

Many Voices.
One Community.

Big Shout out to ADP Core Team

**Rick Ekeland, Muthu Balaraman, Prateek Mishra,
Gilad Ofir, Daniel Casas, Shariful Islam, Kyle Cronin, Jeff Woods,
Swathy Purushothaman, Sameer Syed, GPT teams**

See you at our Birds of Feather session - BOF2-M06

2:20 pm PST (Today)